

UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

FILED

Asheville

Jan 26 2021

U.S. District Court
Western District of N.C.

In the Matter of the Search of

ONE BLACK ALCATEL CELLULAR PHONE, ONE
 AMAZON FIRE TABLET AND ONE HEWLETT
 PACKARD LAPTOP THAT ARE CURRENTLY
 LOCATED AT THE HSI HENDERSONVILLE, NC
 OFFICE LOCATED AT 518 6TH AVENUE WEST,
 HENDERSONVILLE, NC 28792

)

Case No. 1:21-mj-5

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment A to the accompanying Affidavit.

located in the Western District of North Carolina, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B to the accompanying Affidavit.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 2252A and 2251

Offense Description
Receipt, Possession, Distribution, and Production of Child Pornography

The application is based on these facts:

See accompanying Affidavit.

- Continued on the attached sheet.
- Delayed notice _____ days (give exact ending date if more than 30 _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Klarisa C. Zaffark
Klarisa C. Zaffark
Applicant's signature

Klarisa C. Zaffark, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P 4.1 by (**telephone**)

Signed: January 26, 2021

W. Carleton Metcalf
W. Carleton Metcalf
United States Magistrate Judge

Date: 1/26/2021

Case 1:21-mj-00005-WCM Document 1-1 Filed 01/26/21 Page 1 of 24

City and state: Asheville, North Carolina

The Hon. W. Carleton Metcalf, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
ASHEVILLE DIVISION

FILED
Asheville
Jan 26 2021

U.S. District Court
Western District of N.C.

IN THE MATTER OF THE SEARCH OF
ONE BLACK ALCATEL CELLULAR
PHONE, ONE AMAZON FIRE TABLET
AND ONE HEWLETT PACKARD LAPTOP
THAT ARE CURRENTLY LOCATED AT
THE HSI HENDERSONVILLE, NC OFFICE
LOCATED AT 518 6TH AVENUE WEST,
HENDERSONVILLE, NC 28792

Case No. 1:21-mj-5

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Klarisa C. Zaffark, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I have been so employed from May 2010, to the present. I am currently assigned to HSI Hendersonville, North Carolina office. As part of my official duties, I have conducted and participated in investigations relating to narcotics smuggling, human smuggling and trafficking, document fraud, and the sexual exploitation of children. I have also received training and instruction in the field of investigating child pornography. As part of

my duties and responsibilities as an HSI Special Agent, I am authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2251, et seq.

3. As a result of training and experience, I am familiar with methods employed by individuals engaged in various illegal activities, including interstate transportation of child pornography. I am also aware from my training and experience that persons engaged in interstate transportation of child pornography typically use false identities and other techniques to disguise themselves and their enterprise. I am further aware, as a result of my training and experience that child pornography is not generally available in retail establishments, even from those which offer other explicit sexual material. Persons who wish to obtain child pornography do so by ordering and/or obtaining it by discreet contact with other individuals and underground businesses that have child pornography collections.

4. This investigation involves the possession of child pornography across state boundary lines through the use of computers and the Internet. All such transmissions must go through Internet Service Providers servers, where the said Internet Service Provider temporarily stores such transmissions.

5. Your Affiant is personally familiar with the facts and circumstances surrounding this investigation, both from her own investigative activities, and from information obtained from other law enforcement officers/agencies.

6. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

7. As more fully described below, your Affiant has probable cause to believe that presently and/or at the time of this warrant's execution, evidence of child pornography, and evidence linking John Wayne DRYSDALE to possession of child pornography will be found inside the following items: one (1) Black Alcatel Cellular Phone (Model:5002C), one (1) Amazon Fire Tablet (Model: M826G), and one (1) Hewlett Packard Laptop (the Devices). These items, I have reason to believe, will contain evidence of the commission of the crime and of certain activities relating to the possession of child pornography in violation of Title 18, United States Code, § 2252A(a)(5)(B), which relates to the knowingly possessing child pornography. Such items are evidence, contraband, the fruits of crime and things otherwise criminally possessed, property designated or intended for use or which is or has been used as the means of committing a criminal offense.

8. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

9. On or about December 11, 2020, the United States Marshals Service (USMS) assigned to the Asheville, North Carolina office was contacted by the USMS assigned to the Minneapolis, Minnesota office referencing a federal probation fugitive identified as John Wayne DRYSDALE (herein referred to as DRYSDALE). DRYSDALE was identified as a registered sex offender who absconded from the District of Minnesota and was believed to have fled to the Western District of North Carolina, resulting in a federal supervised release violation.

10. DRYSDALE was identified as being previously arrested in 2005 and convicted in

2006 of 18 USC 2113(a)-Bank Robbery, 18 USC 2252A(a)(2)(A)-Receiving Child Pornography, and 18 USC 2252A(a)(5)(B)-Possession of Child Pornography. DRYSDALE was subsequently mandated to the custody of the Bureau of Prisons for one hundred and thirty-nine (139) months, placed on supervised release for a term of Life and mandated to register as a sex offender.

11. USMS Minneapolis conducted investigative inquiries into DRYSDALE's possible whereabouts which resulted in a suspected location of 5025 US Highway 221 S, Forest City, North Carolina 28043.

12. On December 11, 2020, Deputies with the USMS Asheville, with the assistance of the Rutherford County Sheriff's Office (RCSO), approached the residence of 5025 US Highway 221 S, Forest City, North Carolina 28043. Upon approach to the residence, investigators spoke with an individual standing outside and confirmed that DRYSDALE was located within the residence. Deputies with the USMS Asheville made entry into the residence and placed DRYSDALE into custody. DRYSDALE was informed of his rights per *Miranda*, which he invoked and requested to have an attorney present for questioning.

13. Investigators conducted consensual interviews of multiple individuals discovered within the residence. The homeowner was identified as Cheryl Baynard (herein referred to as Cheryl) who stated that she believed DRYSDALE was a friend of her son, Jeff Baynard. Cheryl informed investigators that her son, Jeff Baynard, traveled to Minneapolis, Minnesota on December 3, 2020, and picked up DRYSDALE and transported him to their home in Forest, City, North Carolina, arriving late on December 4, 2020. Cheryl stated she believed DRYSDALE had fallen on hard times and requested a room for rent through the month of January 2021. Cheryl stated she observed DRYSDALE arrive at her home with numerous personal items to include electronic devices.

14. Cheryl provided investigators with consent to enter her home and escorted them to the living room and dining room area where she indicated DRYSDALE's personal items were located. Cheryl escorted investigators to the dining room area where she retrieved one (1) Black Alcatel Cellular Phone (Model: 5002C), one (1) Amazon Fire Tablet (Model: M826G), and one (1) Hewlett Packard Laptop, which she identified as belonging to DRYSDALE, and turned them over to USMS Deputy Bob Spangler.

15. During her interview with Deputy Marshal Spangler, Cheryl stated, "I found something, and I didn't know who it belonged to and I was trying to find out." Cheryl handed Deputy Marshal Spangler a SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594) and stated, "it's not pleasant." Cheryl explained that her grandson, Jasper Baynard (herein referred to as Jasper), located the SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594) in the home and thought it belonged to him and plugged the electronic item into his personally owned desktop computer to review the digital files. Cheryl explained that her grandson, Jasper, observed a digital file that he believed depicted child pornography involving a minor boy. Cheryl handed the SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594) to Deputy Marshal Spangler who then turned over the device to Rutherford County Detectives for seizure processing.

16. RCSO Sergeant Chad Murray approached an adult male standing outside of the residence who identified himself as Jasper. Jasper informed investigators that he discovered the device and explained that he plugged the SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594) into his personally owned desktop computer to review the digital files. Jasper explained that he observed approximately seven (7) or eight (8) folders, one of which was labeled "Boys." Jasper explained he then opened the folder labeled "Boys" and observed

numerous video files. Jasper stated he opened one (1) video file and viewed only a few seconds and immediately knew the file to depict child pornography. Jasper described observing an adult male orally copulating a young boy's penis. Jasper approximated the age of the male child in the video to be eight years-old. Jasper stated he immediately closed the video file and removed the SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594) from his computer and turned it over to his grandmother, Cheryl. RCSO Sergeant Murry requested consent to seize the desktop computer utilized by Jasper to review the digital files found on the SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594). Jasper provided investigators with consent to seize his personally owned desktop computer, identified as a Black Desktop Computer, so that it may be forensically analyzed for evidence of child exploitation material.

17. RCSO Sergeant Murray continued his investigation and made contact with an adult male who identified himself as Jeff Baynard (herein referred to as Jeff). Jeff explained that he met DRYSDALE several years back during truck driving school and became friends. Jeff stated he and DRYSDALE kept in communication via phone calls or Facebook Messenger. Jeff stated that DRYSDALE explained to him that he was out of work and that due to COVID-19, he had fallen on hard times and needed a place to stay. Jeff stated DRYSDALE asked for his help to which he agreed, and that DRYSDALE had paid for his gasoline. Jeff stated that he traveled to a Day's Inn Motel located in St. Paul Minnesota and picked-up DRYSDALE on December 3, 2020. Jeff stated he observed DRYSDALE with personal items such as a backpack, trash bag of clothes, computer, tablet and a cellular phone. RCSO Sergeant Murray asked Jeff if he had seen DRYSDALE in possession of the SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594), to which he nodded no. RCSO Sergeant Murray presented Jeff with the items previously identified by Cheryl as belonging to DRYSDALE. Jeff positively identified the Black

Alcatel Cellular Phone (Model: 5002C), Amazon Fire Tablet (Model: M826G), and Hewlett Packard Laptop as belonging to DRYSDALE.

18. RCSO investigators subsequently seized the SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594) and the Devices identified by both Cheryl and Jeff as belonging to DRYSDALE.

19. On December 18, 2020, HSI Hendersonville agents traveled to RCSO and took custody of the SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594) and the Devices believed to be the property of DRYSDALE.

20. DRYSDALE was taken into custody on December 11, 2020 and transported to the Rutherford County Jail where he has been continuously held pending State of North Carolina charges for violation of sex offender registration.

21. On January 12, 2021, SA Zaffark applied for, and was granted a federal search warrant by the Honorable United States Magistrate Judge William Carleton Metcalf, of the Western District of North Carolina. The search warrant was issued authorizing the search of a SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594) believed to belong to DRYSDALE.

22. The execution of the search warrant was conducted by an HSI forensics analyst who discovered numerous items of evidentiary value. A forensic review revealed the SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594) contained numerous folders comprised of digital artifacts.

23. One folder was discovered labeled "BoyLovers" and contained two (2) digital images depicting child exploitation material. One (1) digital image file was identified as follows:

File Name: 154A7858

File Size: 939 KB

The digital image depicts two (2) prepubescent boys, approximately two (2) to four (4) and five (5) to seven (7) years of age, laying fully nude while on a blue folding beach chair. Both prepubescent boys are depicted nude and exposing their penis and genital areas.

24. One folder was discovered labeled “Boys” and contained two (2) digital videos depicting child exploitation material. One (1) digital video file was identified as follows:

File Name: 2d572908-d3c3-4324-b1c8-2867df3502f4

File Size: 5.82MB

File Length: One minute and thirty-five seconds (01:35)

The video begins depicting an adult male, wearing a yellow shirt and black shorts, orally copulating a pubescent minor boy. The pubescent minor boy appears to be approximately eleven (11) to thirteen (13) years of age and is depicted laying down while fully nude. At approximately forty seconds (00:40) the adult male is observed switching places with the minor boy and begins to remove his shorts, thus exposing his penis. At approximately forty-seven seconds (00:47) the adult male is observed grabbing the minor nude boy and laying him on top of the adult male. The adult male is observed rubbing his hands up and down the minor boys back and exposed buttocks. At approximately one minute and nineteen seconds (01:19) the minor boy is observed utilizing his hand to masturbate the adult male.

25. One folder was discovered labeled “Documents” and contained numerous digital files depicting personal documents associated to DRYSDALE. Among the discovered documents were the following:

File Name: “Bank Statement”

Document Type: Microsoft Word Document

A review of the document revealed a “Wells Fargo Everyday Checking” bank statement dated August 27, 2020. The document appeared to be five (5) pages and depicted the account statement was for account holder John W. Drysdale. The document depicted a statement period activity summary for dates between July 30, 2020 through August 27, 2020. A review of the withdraws and purchases conducted during the above timeframe revealed numerous transactions occurred in Saint Paul, Minnesota.

File Name: “ViewCheckPDF”

Document Type: Portable Document Format (PDF)

A review of the document revealed a wages and earnings statement for John Drysdale dated October 31, 2020. The document appeared to be one (1) page from a company named “Team Personal¹” with assigned address of 259 University Avenue West., Ste. A, Saint Paul, MN 55103. The document listed earnings for hours worked from October 26, 2020 through October 31, 2020 with an assigned company name of “Meyers Printing C². ”

¹ A review of Team Personal’s website revealed the company provides light industrial staffing solutions for several industries.

² A review of The Meyers Printing Companies website revealed it is a printing service company that designs and manufactures signage, labels, case and 3D displays to support retail marketing. The Meyers Printing Companies is based in Minneapolis, MN.

File Name: "Invoice COMMX"

Document Type: Portable Document Format (PDF)

A review of the document revealed an invoice from "Digitstore24³" to John Drysdale at 766 University Avenue West., Saint. Paul, MN 55104. The invoice was dated November 7, 2020 and detailed the purchase of a "Commission Plan X- Membership."

26. As a condition of DRYSDALE's supervised release from the District of Minnesota, he is not permitted to "possess or use a computer or have access to any on-line service without the prior approval of the U.S. Probation and Pretrial Services Office." After consulting with DRYSDALE's supervising U.S. Probation Officer it was confirmed that the U.S. Probation and Pretrial Services Office was not aware of DRYSDALE's possession of the black Alcatel Cellular Phone (Model: 5002C), Amazon Fire Tablet (Model: M826G), or Hewlett Packard Laptop, and that he was not authorized by that office to possess or use those devices.

27. Based on the child pornography digital files and the user attribution documents discovered as a result of a forensic examination conducted on the SanDisk Cruzer Glide 32GB USB (Serial Number: BM2007581594), investigators believe that there is probable cause that presently and/or at the time of this warrant's execution, evidence of child pornography will be found on the Devices. Investigators believe there is evidence linking John Wayne DRYSDALE to possession of child pornography and that evidence of child pornography will be found on the Devices.

³ A review of the Digistore24 website revealed is an online retailer for manufacturers of mainly digital products. Digistore24 processes the sales of ebooks, online memberships, software and seminars.

28. The Devices are currently in evidence storage at HSI Hendersonville, located at 518 6TH Avenue West, Hendersonville, North Carolina 28792. In my training and experience, I know that the device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the HSI.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some

GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

30. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices, and/or other electronic devices that can be attributed to them.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to [[obtain unauthorized access to a victim electronic device over the Internet]], the individual’s electronic device will generally serve both as an instrumentality for committing the crime,

and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

34. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

35. Based on the foregoing facts, I respectfully submit that there is probable cause to believe that evidence of child pornography, and other evidence of the use of computers and/or additional electronic devices to possess child pornography as set forth in the search warrant, will be found on

36. Your Affiant respectfully requests that a warrant be issued authorizing HSI Special Agents, with appropriate assistance from other law enforcement personnel and/or agencies to search the above referenced items.

Reviewed by Special Assistant United States Attorney Alexis Solheim.

/S/ Klarisa C. Zaffark
Date: January 26, 2021
Special Agent
Homeland Security Investigations

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 26th day of January, 2021, at 1:26 PM.

Signed: January 26, 2021



W. Carleton Metcalf
United States Magistrate Judge



ATTACHMENT A

The property to be searched is a Black Alcatel Cellular Phone (Model:5002C), an Amazon Fire Tablet (Model: M826G), and a Hewlett Packard Laptop. The Devices are currently located at HSI Hendersonville, located at 518 6th Avenue West, Hendersonville, North Carolina 28792.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 2252A (a)(5)(B), and) and involve John Wayne DRYSDALE including:
2. All electronic files containing child pornography and images of child pornography in any form, information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 and records or other items which evidence ownership or use of computer that is currently saved on one (1) Black Alcatel Cellular Phone (Model:5002C), one (1) Amazon Fire Tablet (Model: M826G), and one (1) Hewlett Packard Laptop.
3. Records, documents, writings, and correspondences with others pertaining to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
4. Any and all, photographs, letters, written narratives and computer text files or electronic matter to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect or possess visual depictions of minors engaged in sexually explicit conduct.
5. Any and all records showing or bearing indicia of the use, ownership, possession, or control of the items described in Attachment A and items contained therein, including visual depictions of minors engaged in sexually explicit conduct, computer equipment, accessories, telephone(s), modem(s), or such records, whether stored on paper, in files, invoices, bills, leases, deeds, permits, licenses, telephone bills, tax receipts, or other documentation, or on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, or storage media.

6. Envelopes, letters, and other correspondence, including, but not limited to, electronic mail, chat logs, IRC logs, ICQ logs, all usage records for distributed file sharing technologies, and electronic messages, offering to distribute and receive visual depictions of minors engaged in sexually explicit conduct, or to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct.

7. Records or other items which evidence ownership or use of computer equipment listed in Attachment A, including, but not limited to, correspondence, sales receipts, and bills for Internet access relating any other Internet service provider, email addresses.

8. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, letters, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

9. Storage combinations, passwords, and paperwork which indicate any other storage containers or facilities that could contain evidence of collection, advertising, transport, distribution, receipt, or possession of child pornography.

10. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

11. For any computer hard drive or other electronic media (hereinafter, “MEDIA”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of user attribution showing who used or owned the MEDIA at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved usernames and passwords, documents, and browsing history;
- b. passwords, encryption keys, and other access devices that may be necessary to access the MEDIA;
- c. documentation and manuals that may be necessary to access the MEDIA or to conduct a forensic examination of the MEDIA.

12. Visual depictions, in whatever form, including digital, of minors engaged in sexually explicit conduct.